FreeBSD下通过PoPToP实现远程访问VPN

对于构建[VPN](http://www.bitscn.com/network/200606/27426.html" \t "_blank)来说，网络隧道(Tunnelling)技术是个关键技术。网络隧道技术指的是利用一种网络协议来传输另一种网络协议，它主要利用网络隧道协议来实现这种功能。   
　　  
　　现有两种类型的网络隧道协议，一种是二层隧道协议，用于传输二层网络协议，它主要应用于构建远程访问虚拟专网(Access VPN)；另一种是三层隧道协议，用于传输三层网络协议，它主要应用于构建企业内部虚拟专网(Intranet VPN)和扩展的企业内部虚拟专网(Extranet VPN)。   
　　  
　　FreeBSD下的PoPToP实现了二层隧道协议中的PPTP(Point to Point Tunneling Protocol)封装，利用它建立远程访问VPN服务，可以替代现有的电话长途拨号访问。   
　　  
　　**一、 环境**   
　　1. 一台PC服务器安装FreeBSD，双网卡连接内外两个网段，内部地址172.16.1.210/24，外部地址为固定合法IP地址。   
　　2. 外地用户PC通过Internet和FreeBSD主机建立VPN连接连入局域网。   
　　  
　　**二、 安装**  
　　# cd /usr/ports/net/poptop   
　　# make; make install   
　　如果执行make不允许安装，编辑当前目录下的Makefile，将forbidden那行注释掉   
　　  
　　**三、 配置**   
　　a、 # vi /etc/syslog.conf，增加一行daemon.debug /var/log/pptpd.log   
　　# kill –HUP (syslogd当前pid)   
　　b、 # vi /etc/ppp/options   
　　lock   
　　debug   
　　auth   
　　+chap # chap认证方式   
　　proxyarp   
　　# vi /etc/ppp/chap-secrets   
　　user \* password \* # 给VPN用户的用户名和密码   
　　# vi /etc/ppp/ppp.conf   
　　loop:   
　　set timeout 0   
　　set device localhost:pptp   
　　set log phase   
　　set dial   
　　set login   
　　# Server (local) IP address, Range for Clients, and Netmask   
　　set ifaddr 172.16.1.210 172.16.1.225-172.16.1.254 255.255.255.0   
　　set server /tmp/loop "" 0177   
　　loop-in:   
　　set timeout 0   
　　allow mode direct   
　　pptp:   
　　load loop   
　　enable proxy   
　　accept dns   
　　# DNS Servers to assign client   
　　set dns 172.16.1.210   
　　# NetBIOS/WINS Servers to assign client   
　　# set nbns 172.16.1.200   
　　set device !/etc/ppp/secure   
　　# vi /etc/ppp/secure   
　　#!/bin/sh   
　　exec /usr/sbin/ppp -direct loop-in   
　　c、 编辑/etc/local/etc/pptpd.conf   
　　speed 115200   
　　option /etc/ppp/ppp.conf   
　　debug   
　　localip 172.16.1.210   
　　remoteip 172.16.1.225-254 # 连接上来的用户从中获取IP   
　　  
　　**四、 运行**   
　　# /usr/local/etc/rc.d/pptpd.sh start 或   
　　# /usr/local/sbin/pptpd &   
　　  
　　**五、 测试**   
　　找个能连接Internet的windows 98se或win2000机器，创建一个VPN连接。服务器地址填FreeBSD的外部合法IP，用户名user，口令password，并禁用数据压缩属性。   
　　注：windows 98se下建立VPN连接需先添加一个微软虚拟适配器，一个拨号适配器。   
　　  
　　**六、 其他**   
　　1、 VPN的连接速度取决于双方(服务器，用户端)接入Internet的速度。   
　　2、 上述设置的PoPToP服务只实现了一个隧道封装，通过该隧道传输的数据并没有加密，所以并非严格意义上VPN连接。   
　　3、 用户通过VPN连接上来后，相当于直接连入你的局域网。出于安全考虑，可以结合FreeBSD的防火墙(如ipf)，设置一些规则来限制分配给VPN用户的那段IP地址的访问范围。   
　　4、 如果连接失败，打开/var/log/pptpd.log、/var/log/ppp.log查看错误纪录。